

American Business Media (ABM) Comments on Privacy Legislation Draft

June 4, 2010

The Honorable Rick Boucher
U.S. House of Representatives
2187 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Cliff Stearns
U.S. House of Representatives
2370 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Boucher and Ranking Member Stearns,

As you know, American Business Media (ABM) is an association of business information providers, delivering business intelligence to industry professionals worldwide. Its 275-plus member companies reach an audience of more than 100 million professionals, represent nearly 6,000 print and online titles and over 1,000 trade shows and account for over \$26 billion in annual revenues. On the web, ABM members specialize in online resources that cater to the Business to Business (B-to-B) information market, primarily serving business and industry users rather than individual consumers on the internet.

ABM's B-to-B focus offers a unique perspective from which to analyze the draft privacy legislation you recently released and our comments are contained herein.

Core Values

ABM's perspective on the information marketplace is predicated on the belief that customer privacy policies should work effectively in two regards. The first is to ensure that customers are informed about how businesses collect, use and share information about them and are provided with a choice not to use the services of businesses with whose practices they do not agree. The second is that collection, use and sharing of information about customers in a manner transparent to the consumer affects a broad range of business enterprises – including the business to business market which is patently different from the business to consumer market. These tenets apply to offline and online collection of covered information and are founded on the premise that the expectation of privacy differs for the business information user. ABM seeks to ensure these basic premises remain, even though requirements of notice and choice may differ depending on the method or location of collection.

With technology advances and an increased demand by business and industry for content publishers to provide pertinent information, ABM members have increasingly turned to targeting technologies to enhance their customers' experience through customized delivery of information, including both the content those publishers develop and the advertisements that would be of most relevance to the customer and that are necessary to support ABM members' business models. However, members' usage of behavioral advertising is only a small percentage compared to the first-party and contextual delivery that ABM is currently engaged in, though the use of this technology in the future is an important aspect of our business growth.

ABM members inform individuals when collecting information, including how they intend to use it, and they give individuals the opportunity to opt out. This arrangement has worked well for ABM members' customers, and as evidenced by customer privacy policies and practices, our businesses go to great

lengths to provide effective customer privacy protections. We continue to believe that such privacy standards allow users to make an informed decision on how they receive advertising and how their data is being used and collected.

Summary of ABM Position

ABM cautions against government regulations that go beyond the threshold of transparency, notice and choice for business users. We urge you to consider the possible, unintended consequences of establishing new requirements for content providers that may disadvantage the innumerable American businesses that rely on business information products and services to receive targeted and customized information solutions.

Specifically, ABM supports the notion that contextual advertising, first party transactions and transactions conducted by another party to effectuate a first party transaction online should be exempt from express or “opt-in” consent requirements. ABM also believes that regulations should not inhibit evolving online technologies that help bring information to business users and should focus instead on the need for users to understand how and why publishers are adopting these enhancements (i.e., to benefit those users).

ABM is opposed to “opt-in” requirements for the offline collection of basic information from individuals wishing to establish business relationships, or acting within an established business capacity, and believes that the offline collection of basic business information, like that found on a business card or other public industry information, should be exempted from the bill.

ABM takes no position on the requirement of express or “opt-in” consent for unaffiliated third party ad networks. However, ABM is opposed to any requirements that are imposed on first parties as a result of exemptions from opt-in requirements for unaffiliated third party ad networks. Specifically, ABM believes that the in-ad notice and preference profile requirements necessary to achieve exemption from “opt-in” for advertisements served by unaffiliated third party ad networks should be the responsibility of the ad network, not the first party publisher.

In summary, ABM supports the core principles strengthening consumer privacy contained in the draft privacy legislation and looks forward to working with you to amend the areas of most concern to ABM. However, we remain concerned with several sections of the bill that could adversely impact the online and offline collection and use of data. ABM also seeks clarification and exemptions on several key issues contained in the draft legislation that are overly broad or unclear. We have outlined details of these questions and concerns as well as amendments to the draft legislation below.

Areas of Concern & Clarification

1) Collection of Information

The draft legislation currently covers both offline and online collection of all information with respect to an individual, including an individual in his or her business capacity. ABM firmly believes that businesses and business information are not afforded privacy rights in the same manner as individuals

acting in their private capacities. ABM further believes that individuals have differing privacy expectations with respect to what they do in their business and professional capacities.¹ For these reasons, ABM is concerned about the effect this legislation may have in creating unprecedented new rights of privacy for a business or individuals within businesses.

That said, ABM believes that balanced requirements can be achieved in this legislation for the collection of information from individuals acting in a business capacity, depending on whether that information is collected offline or online. Specifically, ABM understands the technological barriers associated with exempting the online collection of information from individuals acting in a business capacity and therefore generally supports the current “opt-out” consent requirements for first party transactions and transactions conducted by another party to effectuate a first party transaction online, notwithstanding some clarifications noted below.

However, ABM believes the proposed opt-in requirements for offline collection and sharing of business information would significantly hamper the flow of business information. ABM also believes that generally mandating privacy notices at all times when covered information is collected offline presents many practical difficulties, and would provide little if any additional useful information to individuals, particularly in business-to-business settings. ABM members currently provide privacy notices offline to inform customers and prospects as to the types of information that is collected and how such information will be used. These notices are also coupled with customer choice to opt-out of further use of the information collected.

For these reasons, we suggest that the offline collection of basic information from persons acting in clear business capacities should be exempted under the bill. The very nature of the offline collection of information allows the capacity of an individual (whether he or she is acting in a professional capacity or a personal capacity) to be easily determined, so a business exemption can be accomplished much more easily than in an online context. At the very least, ABM believes there should be a variation of a “business card” exception – that is, the information normally found on a business card or related to professional services or other public occupational and industry information should not be subject to the opt-in rules or other requirements when collected offline. One note is that we do not suggest that the business exception be based on whether a home or office address is used, since in many areas, including the agricultural and medical fields, home addresses are often used for business purposes.

2) General opt-out rule - Section 3(a)(3)(A)

ABM agrees that the general rule for consent to use of non-sensitive information by first parties and their service providers and affiliates online should be an opt-out rule. Once consumers have provided

¹ “[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy.” *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *see also* Restatement (Second) of Torts § 652I cmt. c (“A corporation, partnership or unincorporated association has no personal right of privacy.”); *Browning-Ferris Indus. v. Kelco Disposal, Inc.*, 492 U.S. 257, 284 (1989) (O’Connor, J., concurring in part, dissenting in part) (“[A] corporation has no ... right to privacy.”). Indeed, the Supreme Court has recognized that “a business, by its special nature and voluntary existence, may open itself to intrusions that would not be permissible in a purely private context.” *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 353 (1977). Moreover, many courts have found that business employees, acting as such, often have lower privacy interests in their business conduct than they would have in their private capacities. *E.g., Curto v. Medical World Communications, Inc.*, 2006 WL 1318387 (E.D.N.Y. 2006) (“Employees expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network.”).

information to a trusted party such as an ABM member, they should be adequately protected by an ability to opt-out of uses of that information as is currently the practice. The opt-out rule works for CAN-SPAM, as incorporated into current FTC guidelines on the issue, and should be the general rule with respect to all uses of information, particularly by trusted first parties.

3) Clarification and Reconsideration of Exemption to Opt-In

a. Contextual and first party advertising

ABM members provide customers with business information content that is highly tailored to the type of business a user is engaged in. Customers seek out certain information sources because they provide them with the greatest value, whether that value derives from the general nature of the information content delivered or from the targeted delivery of content based on stated or observed user interaction with that content. In this regard, a significant portion of advertising revenue is derived from contextual advertising, or advertising that is served to a user based purely on the content of a specific website, webpage or type of business. The current privacy legislative draft does not mention contextual advertising and ABM seeks to clarify whether contextual advertising will be considered covered information. ABM believes that contextual advertising does not involve the collection of any covered information from a user and thus should not be included as transaction regulated by this legislation.

ABM members, as content providers, collect and use information from customers to deliver advertising and content to them. This delivery of contextual advertising and content often requires the usage of cookies or IP addresses, which is considered “covered information” under the discussion draft. Expanding the definition of covered information to include defining an IP address would make it extremely difficult to continue, as B-to-B content providers, to serve relevant content or even contextual first-party advertising. Allowing a consumer to an ABM publication to opt-out of all usages of covered information, including IP addresses, would pose a great danger to the ad-based models currently used by every major publisher. While users may at first find this change in law and practice less “intrusive,” it would not be long before B-to-B publishers would no longer be able to support the very services they now provide. Advertising has long been and will continue to be a revenue source which is essential in providing content in the first place. Due to this concern, we strongly support the exclusion of first-party online advertising, including specific contextual advertising, from this legislation.

b. Coverage of Affiliated Websites - Section 2 (7) A vi – Page 5-6

ABM strongly supports the notion, contained in the bill, that first party transactions include those conducted on all affiliate websites under a common parent company or entity. ABM members often publish information and content on varied topics across multiple websites. Given that one parent company controls all such affiliated websites and sets one privacy policy to cover all affiliated websites, ABM believes that covered information can be collected on any affiliated site and then used across the spectrum of affiliated websites of a single parent company to serve advertisements to a user, as long as users are informed that such practices are being employed by the parent company and its affiliates. ABM further believes that this practice constitutes a first party transaction.

c. Transfer of information to third parties

Requiring opt-in consent prior to data transfer to or from third parties – either offline or online – presents one of the most significant issues with the bill for our members. Requiring the use of only opt-in lists would severely affect the acquisition of new customers, drastically reduce the effectiveness of direct marketing and list rental revenue, and adversely impact an important economic sector. Buyers Guides and other readily available lists that are of great value to both individuals and businesses seeking specific types of suppliers would be greatly impacted by opt-in requirements as they would contain far less data available for marketing purposes.

A marketing list is an aggregate collection of marketing data comprised of individuals who responded to an offer and/or information compiled from a public source. Requiring opt-in consent from each individual maintained in a database would require unknown burdens on the part of our members and generated numerous questions as to how this could be accomplished. In the offline world, for instance, conference or exhibition sponsors collect information on attendees to be made available to exhibitors and other attendees. Our members would need clarification as to what may constitute opt-in consent, for example, whether the use of a pre-checked box indicating that information may be made available to other marketers would be considered as sufficient. We presume that members might be able to obtain consent when conference attendees register for a conference and urge clarification on that matter.

d. Lack of need for opt-in consent

The existing model, both offline and online, of providing notice and opt-out have been working very well in allowing those who are not interested in receiving additional marketing offers from unaffiliated third parties to exercise that preference by opting out of all collection of information about them. We surmise that most individuals would simply not take the active step of opting-in to have their information transferred to others, and thus would not receive relevant messages and offers about products and services in which they may well be interested. Further, it is an industry standard that customer lists are only made available to other reputable businesses and only upon review of the marketing promotion, and most ABM members make it clear to customers that they endeavor to ensure third parties abide by the same notice and choice standards that ABM members make known to their customers. Again, interference with this model would drastically alter the marketing landscape and be counterproductive to commerce.

e. Safe Harbor Exemption for certain third party advertising – Section 3(e)

While the safe harbor provision of section 3(e) looks to affect advertising networks placing ads on third-party websites, it could, as currently drafted, place the compliance obligation on the publisher or content provider and related liability if the safe harbor provisions are violated. This safe harbor provision should be revised to place the obligation of such in-ad notice and offering of a profile preference strictly on the advertising networks that collect or receive covered information. We believe the draft legislation should be amended to place the obligation on the advertising network, including an opt-out choice, profile preference management, and in-ad notice outside of a first-party relationship. An advertising network using tracking technology, cookies or IP addresses should not place liability on an unaffiliated publisher, especially if that publisher does not have access or use the information collected for the ad network itself.

4) Definition of “Transactional Purpose” and “Operational Purpose” - Section 2(7) and 2(12)

While information collected for “transactional” and “operational” purposes are exempt from the bill, the definitions of these key terms are important and should be further defined within the legislation. Indeed, the “transactional purpose” definition is somewhat circular, as it includes within it the key and undefined term “transaction.” It is not clear to ABM members whether many of their ordinary business transactions would be covered by the “transactional purpose” exemption or if the purchasing of goods is a typical covered “transaction.” However, many business transactions today increasingly involve services, many of which involve providing valuable business information to the customer. For example, when an ABM member company produces a trade show, and a business signs up to attend the trade show, that should be viewed as a transaction, so that exchanges and sharing of information collected from the attendees at the trade show fall within the transactional exemption.

5) Clarification of Privacy Guidelines

As written, the legislation imposes additional requirements on the content of Privacy Notice that have raised concerns related to notice and collection.

a. Notification of Material Changes

Specifically including the process by which individuals are notified of material changes in privacy practices and obtaining their express affirmative consent before making such changes is unworkable and unnecessary. Members question how they would determine who would need to be notified (e.g., based on who provided information previously under which notice), and how they would obtain consent. Most members’ Privacy Notices contain a current date or date of last update, which serves to indicate that changes may have been made since the previous iteration, and if prominently displayed, already provide customers with notice of changes that may affect their willingness to continue allowing collection and use of their information as stated in the privacy policy.

b. Exemptions from Notice for Basic Name, Address, Phone and Email Information -- section 3(a)(5)(A)(ii)(II)

While the draft bill recognizes that collection of an individual’s name, address, phone number and email address (hereafter, “Basic Information”) should generally not be hampered with notice requirements, the bill’s treatment of Basic Information is worded in a way that may inappropriately restrict collection and use of Basic Information. Specifically, under section 3(a)(5)(A)(ii)(II), notice is not required when Basic Information is collected as “part of a first party transaction,” meaning, under the definition in section (2)(6), information collected *either on a website or at a place of business*. This is an unnecessarily restrictive exemption for use of Basic Information. Wherever Basic Information is found or collected by a business with which a current or potential customer has indicated a desire to engage, even outside of a website or a business premises, no notice should be required. If, for example, Basic Information is collected by a business at a trade show, no notice should be required, because of the non-private nature of Basic Information. It is, after all, information that is that has long been regularly published in phone directories, with the exception of email addresses, which are essentially the modern counterpart of phone numbers. A blanket exemption of any collection of Basic Information from the

notice provisions of the bill, without the limitation in section 3(a)(5)(A)(ii)(II) to collection as “part of a first party transaction,” would be most appropriate.

c. Length of time that information is retained in identifiable form

The Privacy Notice would require informing readers as to the length of time information is retained in identifiable form. This requirement ignores the fact that businesses may find a need to retain identifiable information for any number of potentially necessary or beneficial purposes and that length of time in which retention of such information to benefit the customer would vary, depending on the purpose. Thus most ABM members – and we would venture to say most businesses – do not have an across-the-board policy for how long customer information is retained. Information may be retained, for instance, depending on companies’ needs to service existing customers as well as to reach out to past customers. Expired subscribers can be offered promotions to renew their subscriptions, for example, and thus become active customers again. Past buyers and conference attendees are among the best prospective future buyers and attendees, and members need to be able to contact such customers past an artificial time period for data retention in order to offer them further value. Additionally, those businesses who offer warranties or may need to recall products would need to be able to access customer records for several years.

d. “Clear and Conspicuous” requirement

ABM seeks clarification on what constitutes notice that is “clearly and conspicuously” posted on the website of a covered entity. ABM members provide clear notice and choice to their users through privacy policies that are clearly linked to their websites homepage. ABM believes the current practice of its members in this manner constitutes privacy policies that are “clearly and conspicuously” posted, but seeks clarification from policymakers to ensure that additional actions will not be required by covered entities that already post or link to privacy policies on their websites.

6) Clarification of Geolocation as Sensitive Information

ABM seeks to clarify the broad definition of precise geolocation contained in Subsection 2(10)(f) as sensitive information that may only be collected with express affirmative consent of the user. In particular, it is necessary for a business to know whether geolocation would include data points such as a zip code, IP address, area code or even mailing address. As mobile and other digital devices are increasingly used to access the internet, ABM member companies are increasingly looking to develop and bring to market products and services to serve subscribers using these devices. In keeping with the demands for timely delivery and relevant business information from users on mobile devices, ABM members may choose to serve advertisements based on the current location of the user. Such a transaction would be conducted by a first party or by another party to effectuate a first party transaction. ABM urges you to carefully consider innovation in serving advertising supported content to mobile devices by clarifying the term “precise geolocation information” to ensure that first party transactions involving the location of a mobile device are exempted from an opt-in requirement.

7) Classification of IP addresses as covered information—Section 2(5)(H)

The current draft of the bill includes Internet Protocol (IP) addresses as “unique personal identifiers” that are generally treated similarly to truly unique personal information such as social security numbers, passport numbers, and customer numbers. However IP addresses do not primarily identify persons. At most, they identify computers, or portals for multiple computers or networks. Given the many benefits from storage and use of IP addresses (everything from speedy delivery of website content to fraud detection), and the significant differences between IP addresses and other true personal identifiers like social security numbers, ABM suggests that this classification may not serve any proper privacy-protection interest and may lead to unintended consequences. One potentially damaging consequence would be the inability of ABM members and other content providers to enforce their intellectual property rights by determining where piracy of their materials has occurred because of customer activities. At the very least, the bill should acknowledge and allow for collection of IP addresses for use in connection with legal proceedings, investigations of crimes or other wrongdoing.

8) Coverage of information obtained from published and public domain sources

ABM understands the bill’s intent to cover all information collected *from* individuals (at least in their non-business capacities). However, the current draft covers as well all information collected *about* individuals, meaning that it covers information obtained from published and public domain sources. The “about” restriction therefore means that it would become unlawful merely to reprint, disseminate, or use certain information that has already been publicly distributed and widely used. Already published information is by nature not private and should not be treated as such. Moreover, serious First Amendment and state-federal preemption issues would be raised by classifying as “private,” or making it unlawful to use, information that is already in the public sphere. *Cf. Cox Publishing Co. v. Cohn*, 420 U.S. 469 (1975) (“...the First and Fourteenth Amendments command nothing less than that the States may not impose sanctions on the publication of truthful information contained in official court records open to public inspection”).

ABM would like to thank you for the opportunity to offer comments to the discussion draft of the privacy legislation prior to its formal introduction and we look forward to working further with you and your staff going forward. Please let us know if you may have any questions or would like additional clarification.

Sincerely,

Gordon Hughes
President, American Business Media